Amendments to the Claims

Please amend the claims as follows:

1. (Currently Amended) An apparatus for sealing a data repository to a trusted computing platform, the apparatus comprising:

an embedded security system (ESS) comprising at least one platform configuration register;

a measurement module configured to generate ~~a~~ one or more measurement values for ~~a~~ one or more devices physically connected to a computer system and to extend the measurement values to at least one platform configuration register; ~~and~~

a key management module configured to seal a cryptographic key associated with a data repository ~~to~~ by cryptographically combining the cryptographic key with the measurement values in at least one platform configuration register, the measurement values representing a trusted configuration of the trusted computing platform, and to unseal the cryptographic key using the measurement values by way of the ESS[[.]]; and

a cryptography module configured to encrypt data stored in the data repository and to decrypt data read from the data repository with the unsealed cryptographic key.

2. (Canceled)

3. (Currently Amended) The apparatus of claim 1, wherein the ESS is a Trusted Platform Module (TPM). ~~in accordance with the Trusted Computing Group computer system specification.~~

4. (Currently Amended) A system for sealing a data repository to a trusted computing platform, the system comprising:

a data repository configured to encrypt data written to the data repository and to decrypt data read from the data repository using a cryptographic key;

an embedded security system (ESS) comprising at least one platform configuration register;

a measuring module configured to generate ~~a~~ one or more measurement value~~s~~ for ~~a~~ one or more device~~s~~ within the system and to extend the measurement value~~s~~ to one of the at least one platform configuration registers; and

a key management module configured to:

seal ~~a~~ the cryptographic key associated with ~~a~~ the data repository ~~to~~ by cryptographically combining the cryptographic key with the at least one platform configuration register measurement value, the measurement value representing a trusted configuration, and to unseal the cryptographic key using the measurement values by way of the ESS[[.]]; and

read a sealed cryptographic key, unseal the cryptographic key, and provide the cryptographic key to the data repository before an operating system loads.

5. (Currently Amended) The system of claim 4, wherein the ESS is a Trusted Platform Module (TPM). ~~in accordance with the Trusted Computing Group computer system specification.~~

6. (Original) The system of claim 4, wherein the key management module is further configured to write the sealed cryptographic key to a non-volatile data repository and to read the sealed cryptographic key from a non-volatile data repository.

7. (Original) The system of claim 6, wherein the non-volatile data repository is a repository selected from the group consisting of an unencrypted partition of a hard drive, a removable device, and a removable media.

8. (Canceled).

9. (Currently Amended) A computer readable storage medium comprising computer readable code configured to carry out a method for sealing a data repository to a trusted computing platform, the method comprising:

encrypting data on a data repository with a cryptographic key;

sealing the cryptographic key by cryptographically combining the cryptographic key with measurement values representing a trusted configuration to a platform configuration to produce a sealed key;

unsealing the sealed key using the measurement values to produce the cryptographic key; and

decrypting data on the data repository with the unsealed cryptographic key.

10. (Currently Amended) The computer readable storage medium of claim [[11]] 9, wherein sealing comprises generating a measurement value for a device comprising the platform configuration and generating the sealed key with the measurement value.

11. (Currently Amended) The computer readable storage medium of claim [[12]] 10, wherein generating a measurement value comprises hashing a code image.

12. (Currently Amended) The computer readable storage medium of claim [[12]] 9, wherein the sealed key is generated with a Trusted Platform Module (TPM).

13. (Currently Amended) The computer readable storage medium of claim [[11]] 9, wherein unsealing comprises decrypting the sealed key with a measurement value for a device comprising the platform configuration, the measurement value matching a measurement value used to produce the sealed key.

14. (Currently Amended) The computer readable storage medium of claim [[15]] 13, wherein a TPM unseals the sealed key.

15. (Currently Amended) The computer readable storage medium of claim [[11]] 9, further comprising storing the sealed cryptographic key in a removable device.

16. (Currently Amended) The computer readable storage medium of claim [[11]] 9, wherein the platform configuration comprises a serial number for the data repository[[,]] .

17. (Currently Amended) The computer readable storage medium of claim [[11]] 9, wherein the platform configuration comprises a decryption module.

18. (Currently Amended) The computer readable storage medium of claim [[11]] 9, wherein the platform configuration comprises firmware and software accessible to a processor without the sealed key.

19. (Currently Amended) A method for sealing a data repository to a trusted computing platform, the method comprising:

encrypting data on a data repository with a cryptographic key;

sealing the cryptographic key by cryptographically combining the cryptographic key with measurement values representing a trusted configuration to a platform configuration to produce a sealed key;

unsealing the sealed key using the measurement values to produce the cryptographic key; and

decrypting data on the data repository with the unsealed cryptographic key.

20. (Currently Amended) The method of claim [[21]] 19, wherein sealing comprises generating a measurement value for a device comprising the platform configuration and generating the sealed key with the measurement value.

21. (Currently Amended) The method of claim [[22]] 20, wherein generating a measurement value for a device comprises hashing firmware code for the device.

22. (Currently Amended) The method of claim [[22]] 20, wherein the sealed key is generated with a Trusted Platform Module (TPM).

23. (Currently Amended) The method of claim [[21]] 19, wherein unsealing comprises decrypting the sealed key with a measurement value for a device comprising the platform configuration, the measurement value matching a measurement value used to produce the sealed key.

24. (Currently Amended) The method of claim [[21]] 19, wherein a TPM unseals the sealed key.

25. (Currently Amended) The method of claim [[21]] 19, further comprising storing the sealed key in a removable device.

26. (Currently Amended) The method of claim [[21]] 19, wherein the platform configuration comprises a serial number for the data repository.

27. (Currently Amended) The method of claim [[21]] 19, wherein the platform configuration comprises a decryption module.

28. (Currently Amended) The method of claim [[21]] 19, wherein the platform configuration comprises firmware and software accessible to a processor without the sealed key.

29. (Currently Amended) An apparatus comprising a logic unit for sealing a data repository to a trusted computing platform, the apparatus comprising:

means for generating a measurement value for a device among a plurality of devices comprising a platform configuration;

means for sealing a cryptographic key associated with a data repository to the measurement value representing the device to produce a sealed key; ~~and~~

means for unsealing the sealed key[[.]]; and

means for decrypting data on the data repository with the unsealed cryptographic key.

30. (Currently Amended) An apparatus for sealing a data repository to a trusted computing platform, the apparatus comprising:

an embedded security system (ESS) comprising at least one platform configuration register and configured to seal a cryptographic key to platform configuration data stored in the at least one platform configuration register to produce a sealed key and further configured to unseal the sealed key to ~~re-~~produce ~~the~~ an unsealed cryptographic key;

a key management module configured to direct the ESS to seal a cryptographic key associated with a data repository ~~to~~ by cryptographically combining the cryptographic key with a measurement value associated with the data repository, the measurement values representing a trusted configuration of the

trusted computing platform, and further configured to manage the sealed key,

a measurement module configured to generate the measurement value for the data repository physically connected to the ESS, the ESS extending the measurement value to the at least one platform configuration register;

a cryptographic module configured to encrypt data stored to the data repository and to decrypt data read from the data repository with the unsealed cryptographic key, and

a removable data repository configured to store the sealed key associated with the data repository.